

# **EnGenius EOC1650**

## **Wireless Access Point & Client Bridge**



# **User's Manual**

Version: 2.0

## Table of Contents

---

<b>1</b>	<b>INTRODUCTION .....</b>	<b>6</b>
1.1	FEATURES .....	6
1.2	PACKAGE CONTENTS .....	7
1.3	SYSTEM REQUIREMENTS .....	7
1.4	APPLICATIONS.....	7
<b>2</b>	<b>UNDERSTANDING THE HARDWARE .....</b>	<b>9</b>
2.1	HARDWARE INSTALLATION .....	9
2.2	HARDWARE DESCRIPTION .....	9
2.3	MOUNTING KITS .....	10
2.4	IP ADDRESS CONFIGURATION .....	10
<b>3</b>	<b>SWITCHING BETWEEN OPERATING MODES.....</b>	<b>12</b>
3.1	LOGGING IN .....	12
<b>4</b>	<b>ACCESS POINT OPERATING MODE .....</b>	<b>13</b>
4.1	LOGGING IN .....	13
4.2	STATUS.....	14
4.2.1	MAIN.....	14
4.2.2	WIRELESS CLIENT LIST .....	15
4.2.3	SYSTEM LOG.....	15
4.3	SYSTEM .....	15
4.3.1	SYSTEM PROPERTIES .....	16
4.3.2	IP SETTINGS .....	16
4.3.3	SPANNING TREE SETTINGS.....	17
4.4	WIRELESS .....	17
4.4.1	WIRELESS NETWORK.....	17
4.4.2	WIRELESS MAC FILTER .....	21
4.4.3	WDS LINK SETTINGS.....	22
4.4.4	WIRELESS ADVANCED SETTINGS .....	22
4.5	MANAGEMENT .....	24
4.5.1	ADMINISTRATION .....	24
4.5.2	MANAGEMENT VLAN.....	24
4.5.3	SNMP SETTINGS .....	25
4.5.4	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS .....	25
4.5.5	FIRMWARE UPGRADE.....	26
4.5.6	TIME SETTINGS .....	26
4.5.7	LOG .....	27
4.5.8	DIAGNOSTICS.....	27
<b>5</b>	<b>CLIENT BRIDGE OPERATING MODE .....</b>	<b>29</b>
5.1	LOGGING IN .....	29
5.2	STATUS.....	30
5.2.1	MAIN.....	30
5.2.2	CONNECTION STATUS.....	30
5.2.3	SYSTEM LOG.....	31
5.3	SYSTEM .....	32
5.3.1	SYSTEM PROPERTIES .....	32
5.3.2	IP SETTINGS .....	32

5.3.3	SPANNING TREE SETTINGS.....	33
5.4	WIRELESS .....	33
5.4.1	WIRELESS NETWORK.....	33
5.4.2	WIRELESS SECURITY .....	34
5.4.3	WIRELESS ADVANCED SETTINGS .....	36
5.5	MANAGEMENT .....	37
5.5.1	ADMINISTRATION .....	37
5.5.2	SNMP SETTINGS .....	38
5.5.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS .....	39
5.5.4	FIRMWARE UPGRADE.....	39
5.5.5	TIME SETTINGS .....	40
5.5.6	LOG .....	40
5.5.7	DIAGNOSTICS.....	40
<b>6</b>	<b>WDS BRIDGE OPERATING MODE .....</b>	<b>42</b>
6.1	LOGGING IN .....	42
6.2	STATUS.....	43
6.2.1	MAIN.....	43
6.2.2	WDS LINK STATUS .....	44
6.2.3	SYSTEM LOG.....	44
6.3	SYSTEM .....	45
6.3.1	SYSTEM PROPERTIES .....	45
6.3.2	IP SETTINGS .....	45
6.3.3	SPANNING TREE SETTINGS.....	46
6.4	WIRELESS .....	46
6.4.1	WIRELESS NETWORK.....	47
6.4.2	WDS LINK SETTINGS.....	47
6.4.3	WDS SECURITY.....	48
6.4.4	WIRELESS ADVANCED SETTINGS .....	48
6.5	MANAGEMENT .....	49
6.5.1	ADMINISTRATION .....	50
6.5.2	SNMP SETTINGS .....	50
6.5.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS .....	51
6.5.4	FIRMWARE UPGRADE.....	51
6.5.5	TIME SETTINGS .....	52
6.5.6	LOG .....	52
6.5.7	DIAGNOSTICS.....	53
<b>7</b>	<b>CLIENT ROUTER OPERATING MODE.....</b>	<b>54</b>
7.1	LOGGING IN .....	54
7.2	STATUS.....	54
7.2.1	MAIN.....	55
7.2.2	DHCP CLIENT TABLE .....	56
7.2.3	CONNECTION STATUS.....	56
7.2.4	SYSTEM LOG.....	57
7.3	SYSTEM .....	58
7.3.1	SYSTEM PROPERTIES .....	58
7.4	ROUTER.....	58
7.4.1	WAN SETTINGS.....	58
7.4.1.1	WAN - DHCP .....	59
7.4.1.2	WAN – STATIC IP .....	59
7.4.1.3	WAN – PPPoE .....	60
7.4.1.4	WAN – PPTP .....	62

---

7.4.2	LAN SETTINGS.....	63
7.4.3	VPN PASS THROUGH.....	63
7.5	WIRELESS .....	64
7.5.1	WIRELESS NETWORK.....	64
7.5.2	WIRELESS SECURITY.....	65
7.5.2.1	WIRELESS SECURITY : WEP .....	65
7.5.2.2	WIRELESS SECURITY : WPA-PSK, WPA2-PSK, .....	66
7.5.3	WIRELESS ADVANCED SETTINGS .....	66
7.6	MANAGEMENT .....	67
7.6.1	ADMINISTRATION .....	68
7.6.2	SNMP SETTINGS .....	68
7.6.3	BACKUP/RESTORE SETTINGS, RESET TO FACTORY DEFAULT SETTINGS .....	69
7.6.4	FIRMWARE UPGRADE.....	70
7.6.5	TIME SETTINGS .....	70
7.6.6	LOG .....	71
7.6.7	DIAGNOSTICS.....	71
<b>APPENDIX A – FCC INTERFERENCE STATEMENT .....</b>		<b>73</b>
<b>APPENDIX B – IC STATEMENT .....</b>		<b>74</b>

## Revision History

---

Version	Date	Remark
1.0	Aug 24, 2008	Initial Version
2.0	Jul 28, 2009	New Feature and Functions Included for firmware v1.0.39

# 1 Introduction

---

EOC1650 is a revolutionary product consists of conciseness, quality, and flexibility. It comes with 7dBi internal antenna and upgradable SMA interface provides a customizable interface for enhanced network coverage. Attached suction cup allows quick installation on window or smooth surface.

Operation mode provides Access Point / Client Bridge / WDS Bridge / Client Router and high bandwidth up to 54Mbps. It features high transmitted output power and high receivable sensitivity. High output power and high sensitivity extends range and coverage to reduce the roaming between Access Points to ensure a stable wireless connection and reduce the expense of equipment.

It supports distance control ranges from 1km to 30km and RSSI indicator which enables the best transmitted and received signals for traffic communication. User can choose a suitable antenna for flexible application. This product comes with PoE injector for building in outdoor environment easily.

To protect wireless connectivity, EOC1650 encrypt wireless transmissions through 64/128-bit WEP data encryption and also supports WPA/WPA2. The MAC address filter lets you select exactly which stations should have access to your network. In addition, the User Isolation function can protect the private network between client users.

The attractive design, high performance, and array of features make EOC1650 an optimal wireless solution choice for your residence and office.

## 1.1 Features

### **Wireless**

- **2.4GHz** It works in 2.4GHz frequency spectrum
- **High output power** Transmit high output power programmable for different country selections
- **High Data Rate** High speed transmitting rate up to 54Mbps, support large payload
- **Multifunction application** Access Point/Client Bridge/Client Router/WDS Function
- **Long range transmitting** Transmit power control and distance control (ACK timeout)
- **Narrow Bandwidth** Provide 5MHz/10MHz/20MHz bandwidth selection
- **Signal Strength Display** RF signal strength status shown LEDs of 3 colors, making network build-up easier. LED indicators have the best transmit and receive signal for traffic communication
- **Multiple SSID** 4 SSID supported. Each SSID can set itself wireless or WAN access setting.
- **QoS(WMM)** Enhance performance and density

### **Networking**

- **PPPoE** Point-to-Point Protocol over Ethernet at Client Router mode. This function will keep trying when failed or disconnected
- **PPTP** Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks
- **VPN Pass Through**

## Security

- **802.11i** WEP, WPA, WPA2 (Encryption support TKIP/AES)
- **MAC address functions** MAC address filter (AP mode)
- **802.1x** IEEE802.1x Authenticator
- **Station isolation**

## Management

- **Firmware Upgrade** Upgrading firmware via web browser, setting are reserved after upgrade
- **Reset & Backup** Reset to factory default. User can export all setting into a file via WEB
- **Ping & Trace Route** Built-in PING function & Trace Route function in Web GUI
- **MIB** MIB I, MIB II(RFC1213), Private MIB
- **SNMP** V1, V2c

## 1.2 Package Contents

Open the package carefully, and make sure that none of the items listed below are missing. Do not discard the packing materials, in case of return; the unit must be shipped in its original package.

- 1\* 802.11b/g Long range AP/CB (EOC1650)
- 1\* PoE injector (EPE-1212)
- 1\* Power Adaptor
- 1\* CD with User's Manual
- 1\* Quick Installation Guide (QIG)
- 1\* Metal Strap
- 2\* Special Screw Set
- 1\* 5dBi Dipole Antenna
- 2\* Suction Cup

## 1.3 System Requirements

The following are the minimum system requirements in order to configure the device.

- PC/AT compatible computer with an Ethernet interface.
- Operating system that supports HTTP web-browser

## 1.4 Applications

The wireless LAN products are easy to install and highly efficient. The following list describes some of the many applications made possible through the power and flexibility of wireless LANs:

### a) *Difficult-to-wire environments*

There are many situations where wires cannot be laid easily. Historic buildings, older buildings, open areas and across busy streets make the installation of LANs either impossible or very expensive.

### b) *Temporary workgroups*

Consider situations in parks, athletic arenas, exhibition centers, disaster-recovery, temporary offices and construction sites where one wants a temporary WLAN

established and removed.

**c) *The ability to access real-time information***

Doctors/nurses, point-of-sale employees, and warehouse workers can access real-time information while dealing with patients, serving customers and processing information.

**d) *Frequently changed environments***

Show rooms, meeting rooms, retail stores, and manufacturing sites where frequently rearrange the workplace.

**e) *Small Office and Home Office (SOHO) networks***

SOHO users need a cost-effective, easy and quick installation of a small network.

**f) *Wireless extensions to Ethernet networks***

Network managers in dynamic environments can minimize the overhead caused by moves, extensions to networks, and other changes with wireless LANs.

**g) *Wired LAN backup***

Network managers implement wireless LANs to provide backup for mission-critical applications running on wired networks.

**h) *Training/Educational facilities***

Training sites at corporations and students at universities use wireless connectivity to ease access to information, information exchanges, and learning.



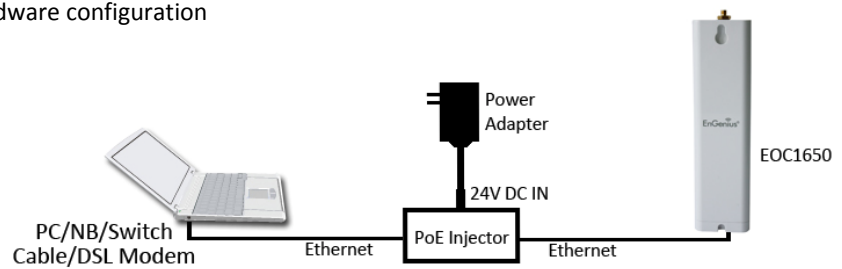
## 2 Understanding the Hardware

---

### 2.1 Hardware Installation

1. Place the unit in an appropriate location after conducting a site survey.
2. Plug one end of the Ethernet cable into the Network port of the PoE injector and another end into your PC/Notebook.
3. Plug one end of another Ethernet cable to AP/Bridge port of the PoE injector and the other end into you cable/DSL modem (Internet)
4. Insert the DC-inlet of the power adapter into the 24V port of the PoE injector and the other end into the power socket on the wall.

This diagram depicts the hardware configuration



### 2.2 Hardware Description

The images below depict the front and rear panel of the unit.

Front Panel



Rear Panel



## 2.3 Mounting Kits

The images below depict the standard mounting kits.

**Pole Mount**



**Wall Mount**



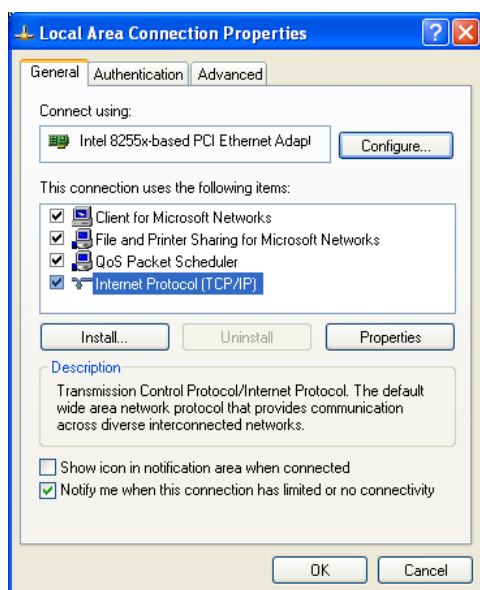
**Window Mount**



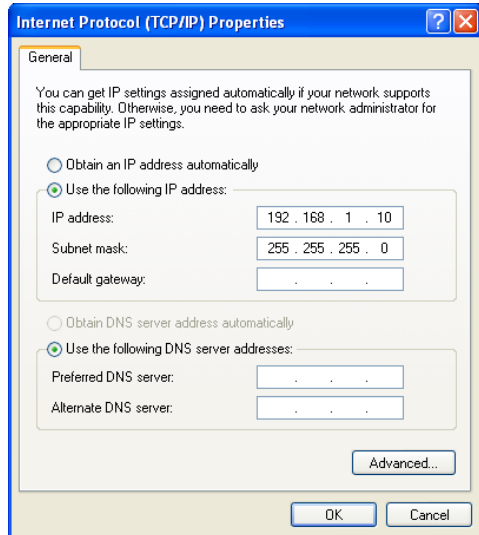
## 2.4 IP Address Configuration

This device can be configured as a **Access Point / Client Bridge / WDS Bridge / Client Router**. The default IP address of the device is **192.168.1.1**. And in order to log into this device, you must first configure the TCP/IP settings of your PC/Notebook.

1. In the control panel, double click Network Connections and then double click on the connection of your Network Interface Card (NIC). You will then see the following screen.



2. Select **Internet Protocol (TCP/IP)** and then click on the **Properties** button. This will allow you to configure the TCP/IP settings of your PC/Notebook.



3. Select **Use the following IP Address** radio button and then enter the IP address and subnet mask. Ensure that the IP address and subnet mask are on the same subnet as the device.  
For Example:

PC IP address: 192.168.1.10

PC subnet mask: 255.255.255.0

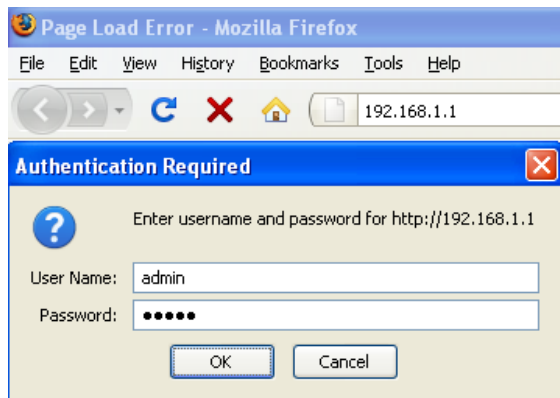
4. Click on the **OK** button to close this window, and once again to close LAN properties window.

## 3 Switching Between Operating Modes

This device can operate in three modes: Access Point, Client Bridge, WDS Bridge and Client Router. This chapter will describe how to switch between operating modes.

### 3.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computer are configured on the same subnet. (Refer to **Chapter 2** in order to configure the IP address of your computer)
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.



- After logging in, you will see the graphical user interface of the device. Click on the **System Properties** link under the **System** navigation drop-down menu.

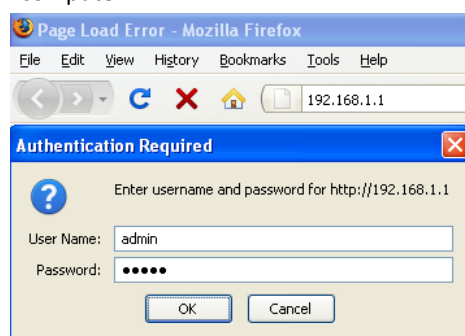
System Properties		Home	Reset
Device Name	Access Point ( 1 to 32 characters )		
Country/Region	Please Select a Country Code		
Operation Mode	<input checked="" type="radio"/> Access Point <input type="radio"/> Client Bridge <input type="radio"/> WDS Bridge <input type="radio"/> Client Router		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- Select operating mode you want from the list (Access Point, Client Bridge, WDS Bridge or Client Router) and then click on the **Apply** button.

## 4 Access Point Operating Mode

### 4.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.
- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:
  1. **Status:** Displays the overall status, connection status, and event log.
  2. **System:** This menu includes the system properties, IP and Spanning Tree settings.
  3. **Wireless:** This menu includes network setting, MAC filter, WDS link, advanced, and security.
  4. **Management:** This menu includes the admin setup, SNMP, firmware upgrade, diagnostics, time setting and save/restore backup.



**EnGenius Wireless Access Point / Client Bridge**

**Access Point**

**Main** [Home] [Reset]

**System Information**

Device Name	Access Point
Ethernet MAC Address	00:02:6f:57:87:0a
Wireless MAC Address	00:02:6f:57:87:0b
Country	N/A
Current Time	Sat Jan 1 00:02:59 UTC 2000
Firmware Version	1.0.39
Management VLAN ID	Untagged

**LAN Settings**

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

**Current Wireless Settings**

Operation Mode	Access Point
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Profile Isolation	No
Profile Settings (SSID/Security/VID)	1 EnGenius1/Open System/No Encryption/1 2 N/A 3 N/A 4 N/A
Spanning Tree Protocol	Disabled
Distance	1 Km

**Navigation Menu:**

- Status**
  - Main
  - Wireless Client List
  - System Log
- System**
  - System Properties
  - IP Settings
  - Spanning Tree Settings
- Wireless**
  - Wireless Network
  - Wireless MAC Filter
  - WDS Link Settings
  - Wireless Advanced Settings
- Management**
  - Administration
  - Management VLAN
  - SNMP Settings
  - Backup/Restore Settings
  - Firmware Upgrade
  - Time Settings
  - Log
  - Diagnostics

## 4.2 Status

### Status

- Main
- Wireless Client List
- System Log

- Click on the **Status** link on the navigation drop-down menu. You will then see three options: Main, Wireless Client List, and System Log. Each option is described in detail below.

### 4.2.1 Main

- Click on the **Main** link under the **Status** drop-down menu. The status that is displayed corresponds with the operating mode that is selected. Information such as Device Name, MAC Address, Country, Current Time and Firmware Version are displayed in the 'System Information' section. IP address, Subnet Mask, and Default Gateway are displayed in the 'LAN Setting' section. In the 'Wireless Settings' section, Operation Mode, Wireless Mode, Channel/Frequency, MSSID with security, Spanning Tree and Distance setting are displayed.

#### Main

[Home](#)[Reset](#)

##### System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:57:87:0a
Wireless MAC Address	00:02:6f:57:87:0b
Country	N/A
Current Time	Sat Jan 1 00:05:22 UTC 2000
Firmware Version	1.0.39
Management VLAN ID	Untagged

##### LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

##### Current Wireless Settings

Operation Mode	Access Point
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Profile Isolation	No
Profile Settings (SSID/Security/VID)	1 EnGenius1/Open System/No Encryption/1
	2 N/A
	3 N/A
	4 N/A
Spanning Tree Protocol	Disabled
Distance	1 Km

[Refresh](#)

### 4.2.2 Wireless Client List

- Click on the **Wireless Client List** link under the **Status** drop-down menu. This page displays the list of Clients that are associated to the Access Point.
- The MAC addresses and signal strength for each client is displayed. Click on the **Refresh** button to refresh the client list.

**Client List**

HomeReset

#	MAC Addr	RSSI(dBm)
---	----------	-----------

Refresh

### 4.2.3 System Log

- Click on the **System Log** link under the **Status** drop-down menu. The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.

**System Log**

HomeReset

Show log type All

Local Log is disabled.

RefreshClear

## 4.3 System

**System**

- System Properties
- IP Settings
- Spanning Tree Settings

- Click on the **System** link on the navigation drop-down menu. You will then see three options: System Properties, IP Settings, and Spanning Tree Settings. Each option is described in detail below.

### 4.3.1 System Properties

- Click on the **System Properties** link under the **System** drop-down menu. This page allows you to switch the operating mode of the device, as well as specify a name and select the operating region.

System Properties		Home	Reset
Device Name	<input type="text" value="Access Point"/> ( 1 to 32 characters )		
Country/Region	<input type="text" value="Please Select a Country Code"/>		
Operation Mode	<input checked="" type="radio"/> Access Point <input type="radio"/> Client Bridge <input type="radio"/> WDS Bridge <input type="radio"/> Client Router		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- Device Name:** Specify a name for the device (this is not the SSID),
- Country/Region:** Select a country from the drop-down list.
- Operating Mode:** Select an operating mode. Configuration for each operating mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

### 4.3.2 IP Settings

- Click on the **IP Settings** link under the **System** drop-down menu. This page allows you to configure the device with a static IP address or a DHCP client.

IP Settings		Home	Reset
IP Network Setting	<input type="radio"/> Obtain an IP address automatically (DHCP) <input checked="" type="radio"/> Specify an IP address		
IP Address	<input type="text" value="19"/> . <input type="text" value="16"/> . <input type="text" value="1"/> . <input type="text" value="1"/>		
IP Subnet Mask	<input type="text" value="25"/> . <input type="text" value="25"/> . <input type="text" value="25"/> . <input type="text" value="0"/>		
Default Gateway	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- IP Network Setting:** Select **Obtain an IP address automatically (DHCP)** radio button if the Access Point is connected to a DHCP server. This will allow the Access Point to pass IP addresses to the clients associated with it. You may select **Specify an IP Address** radio button if you would like the device to use a static IP address. In this case, you would be required to specify an IP address, subnet mask, and default gateway IP address.
- IP Address:** Specify an IP address
- IP Subnet Mask:** Specify the subnet mask for the IP address
- Default Gateway:** Specify the IP address of the default gateway.
- Click on the **Apply** button to save the changes.



4.3.3 Spanning Tree Settings

- Click on the **Spanning Tree** link under the **System** drop-down menu Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

Spanning Tree Settings

HomeReset

Spanning Tree Status	<input type="radio"/> On <input checked="" type="radio"/> Off
Bridge Hello Time	<input type="text" value="1"/> seconds (1-10)
Bridge Max Age	<input type="text" value="20"/> seconds (6-40)
Bridge Forward Delay	<input type="text" value="4"/> seconds (4-30)
Priority	<input type="text" value="32768"/> seconds (0-65535)

Apply

Cancel

- **Spanning Tree Status:** Choose to enable or disable the spanning tree feature.
- **Bridge Hello Time:** Specify the number of seconds for the hello time.
- **Bridge Max Age:** Specify the number of seconds for the max age.
- **Bridge Forward Delay:** Specify the number of seconds for the bridge forward delay.
- **Priority:** Specify the number of seconds for the priority.
- Click on the **Apply** button to save the changes.

4.4 Wireless

Wireless

- Wireless Network
- Wireless MAC Filter
- WDS Link Settings
- Wireless Advanced Settings

- Click on the **Wireless** link on the navigation drop-down menu. You will then see four options: wireless network, wireless MAC filter, WDS link settings, and wireless advanced settings. Each option is described below.

4.4.1 Wireless Network

- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.

## Wireless Network

Home

Reset

Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)			
Channel / Frequency	Ch1-2.412GHz			
Current Profiles				
SSID	Security	VID	Enable	Edit
EnGenius1	Open System/No Encryption	1	<input checked="" type="checkbox"/>	Edit
EnGenius2	Open System/No Encryption	2	<input type="checkbox"/>	Edit
EnGenius3	Open System/No Encryption	3	<input type="checkbox"/>	Edit
EnGenius4	Open System/No Encryption	4	<input type="checkbox"/>	Edit
Profile (SSID) Isolation		<input checked="" type="radio"/> No Isolation <input type="radio"/> Isolate all Profiles (SSIDs) from each other using VLAN (802.1Q) standard		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>				

- **Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **B, G or B/G-mixed**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.
- **Channel / Frequency:** Select a channel from the drop-down list. The channels available are based on the country's regulation.
- **Current Profiles:** User can setup SSID configuration in this item. EOC1650 supports 4 SSIDs, user can decide to use how many SSID via "Enable" or not. When click "Edit" button, you can setup detail, include SSID, VLAN ID and Security Mode.

## SSID Profile

Wireless Setting	
SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Wireless Security	
Security Mode	Disabled
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

## ► Wireless Security – Security Mode : WEP

## SSID Profile

### Wireless Setting

SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

### Wireless Security

Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	<input checked="" type="checkbox"/> 40/64-bit (10 hex digits or 5 ASCII char) <input type="checkbox"/> 104/128-bit (26 hex digits or 13 ASCII char) <input type="checkbox"/> 128/152-bit (32 hex digits or 16 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

►► **Security Mode:** Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.

►► **Authentication Type:** Select an authentication method. Options available are **Open Key**, **Shared Key**. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the Access Point. The device requesting authentication encrypts the challenge text and sends it back to the Access Point. If the challenge text is encrypted correctly, the Access Point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.

►► **Input Type:** Select Hex or ASCII from the drop-down list

►► **Key Length:** Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F and a through f.

►► **Default Key:** You may use up to four different keys for four different networks. Select the current key that will be used.

►► **Key 1-4:** You may enter four different WEP keys.

►► Click on the **Save** button to save the changes.

### ► Wireless Security – Security Mode : WPA-PSK, WPA2-PSK, WPA-PSK Mixed

## SSID Profile

### Wireless Setting

SSID	EnGenius1	(1 to 32 characters)
VLAN ID	1	(1~4095)
Suppressed SSID	<input type="checkbox"/>	
Station Separation	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

### Wireless Security

Security Mode	WPA-PSK	
Encryption	Auto	
Passphrase	passphrase1	(8 to 63 characters) or (64 Hexadecimal characters)
Group Key Update Interval	3600	seconds(30~3600, 0: disabled)

►► **Security Mode:** Select **WPA-PSK**, **WPA2-PSK**, or **WPA-PSK Mixed** from the drop-down list if your wireless network uses WPA pre-shared key.

►► **Encryption:** Select **TKIP** or **AES** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.

►► **Passphrase:** Specify a passphrase that is shared amongst the Access Points and clients.

►► **Group Key Update Interval:** Specify the number of seconds after which the Access Point will probe the client for the passphrase.

►► Click on the **Save** button to save the changes.

### ► Wireless Security – Security Mode : WPA, WPA2, WPA Mixed

## SSID Profile

### Wireless Setting

SSID	EnGenius1 (1 to 32 characters)
VLAN ID	1 (1~4095)
Suppressed SSID	<input type="checkbox"/>
Station Separation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

### Wireless Security

Security Mode	WPA
Encryption	Auto
Radius Server	0 . 0 . 0 . 0
Radius Port	1812
Radius Secret	secret1
Group Key Update Interval	3600 seconds(30~3600, 0: disabled)

►► **Security Mode:** Select **WPA**, **WPA2** or **WPA Mixed** from the drop-down list if your wireless network uses WPA. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.

►► **Encryption:** Select **TKIP** or **AES** from the drop-down list if your wireless network uses this encryption.

►► **RADIUS Server:** Enter the IP address of the RADIUS server.

►► **RADIUS Port:** Enter the port number of the RADIUS server. The default is usually 1812.

►► **RADIUS Secret:** Enter the shared password of the RADIUS server.

►► **Group Key Update Interval:** Specify the number of seconds after which the Access Point will probe the client for the secret.

►► Click on the **Save** button to save the changes.

- **Profile (SSID) Isolation:** When you select this function to enable, unit can isolate all profiles(SSIDs) from each other using VLAN standard.

### 4.4.2 Wireless MAC Filter

- Click on the **Wireless MAC Filter** link under the **Wireless** menu. On this page you can filter the MAC address by allowing or blocking access the network.

Wireless MAC Filter

Home

Reset

ACL Mode 

Disabled

:::::

Add

#	MAC Address

Apply

- **ACL (Access Control) Mode:** You may choose to **Disable**, **Allow Listed**, or **Deny Listed** MAC addresses from associating with the network. By selecting **Allow MAC in the List**, only the address listed in the table will have access to the network; all other clients will be blocked. On the other hand, selected **Deny MAC in the List**, only the listed MAC addresses will be blocked from accessing the network; all other clients will have access to the network.
- **MAC Address:** Enter the MAC address.
- This table lists the blocked or allowed MAC addresses; you may delete selected MAC address or delete all the addresses from the table by clicking on the **Delete** button.
- Click on the **Apply** button to save the changes.









### 4.4.3 WDS Link Settings

Click on the **WDS Link Settings** link under the **Wireless** menu. On this page you can set the WDS link to connect to another WDS AP or WDS Bridge. The Maximum connection is up to 8 units.

WDS Link Settings

HomeReset

**Notice:** When using this WDS Link Settings feature, please disable isolation feature first in Wireless Network page.

ID	MAC Address	Mode
1	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable 
2	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable 
3	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable 
4	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable 
5	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable 
6	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable 
7	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable 
8	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>	Disable 

Apply

Cancel

#### 4.4.4 Wireless Advanced Settings

- Click on the **Wireless Advanced Settings** link. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, fragmentation threshold, RTS threshold, protection mode and distance.

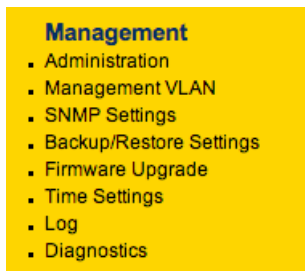
**Wireless Advanced Settings**[Home](#)[Reset](#)

Data Rate	Auto
Transmit Power	20 dBm
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	1 km

[Apply](#)[Cancel](#)

- **Data Rate:** If you would like to force a data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Transmit Power:** You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **Fragment Length:** Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS/CTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Protection Mode:** If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **WMM:** Enable wireless Quality of Service
- **Distance (1-30km):** Specify a distance between 1 and 30Km.
- **Channel Bandwidth:** For different application, you can select 20MHz, 10MHz or 5MHz channel bandwidth.
- Click on the **Apply** button to save the changes.

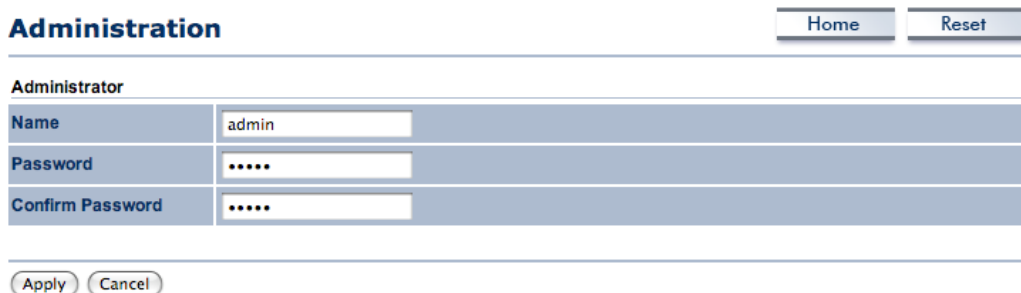
## 4.5 Management



- Click on the **Management** link on the navigation drop-down menu. You will then see seven options: administration, SNMP settings, backup/restore settings, firmware upgrade, time settings, and log. Each option is described below.

### 4.5.1 Administration

- Click on the **Administration** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.



**Administration** Home Reset

Administrator

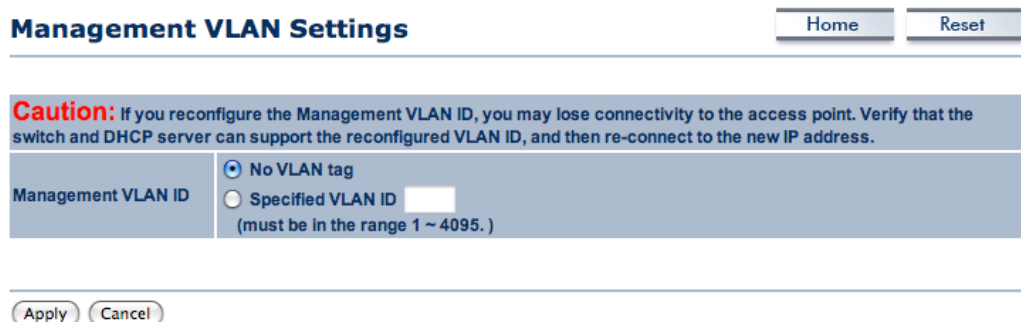
Name	admin
Password	.....
Confirm Password	.....

Apply Cancel

- Name:** Specify a user name into the first field.
- Password:** Specify a password into this field and then re-type the password into the **Confirm Password** field.
- Click on the **Apply** button to save the changes.

### 4.5.2 Management VLAN

- Click on the **Management VLAN** link under the **Management** menu. This option allows you to specify VLAN ID(From 1 to 4095). ( Caution : If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify the switch and DHCP server can support the reconfigured VLAN ID, and then reconnect to new IP address )



**Management VLAN Settings** Home Reset

**Caution:** If you reconfigure the Management VLAN ID, you may lose connectivity to the access point. Verify that the switch and DHCP server can support the reconfigured VLAN ID, and then re-connect to the new IP address.

Management VLAN ID	<input checked="" type="radio"/> No VLAN tag <input type="radio"/> Specified VLAN ID <input type="text"/> (must be in the range 1 ~ 4095. )
--------------------	---

Apply Cancel



- **Name:** Specify a user name into the first field.
- **Password:** Specify a password into this field and then re-type the password into the **Confirm Password** field.

Click on the **Apply** button to save the changes.

### 4.5.3 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.

SNMP Settings		Home	Reset
SNMP Enable/Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
Contact	<input type="text"/>		
Location	<input type="text"/>		
Community Name (Read Only)	<input type="text" value="public"/>		
Community Name (Read/Write)	<input type="text" value="private"/>		
Trap Destination IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>		
Trap Destination Community Name	<input type="text" value="public"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- **SNMP Enable/Disable:** Choose to **enable** or **disable** the SNMP feature.
- **Contact:** Specify the contact details of the device.
- **Location:** Specify the location of the device.
- **Read-Only Community Name:** Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name:** Specify the password for access to the SNMP community with read/write access.
- **Send SNMP Trap:** Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Community Name:** Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

### 4.5.4 Backup/Restore settings, Reset to factory default settings

- Click on the **Backup/Restore Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.

## Backup/Restore Settings

[Home](#)[Reset](#)

Save A Copy of Current Settings

Backup

Restore Saved Settings from A File

選擇檔案 尚未選取檔案

Restore

Revert to Factory Default Settings

Factory Default

- **Save a copy of the current settings:** Click on the Backup button to save the current configuration.
- **Restore saved settings from a file:** Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings:** Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: 192.168.1.1

### System Rebooting...

Rebooting, Please wait... [Click here when AP is ready](#)

## 4.5.5 Firmware Upgrade

- Click on the **Upgrade Firmware** link under the **Management** menu. This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.

## Firmware Upgrade

[Home](#)[Reset](#)

Current firmware version: 1.0.39

Locate and select the upgrade file from your hard disk:

選擇檔案 尚未選取檔案

Upgrade

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** button.  
**Note:** The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

## 4.5.6 Time Settings

- Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.

## Time Settings

[Home](#)[Reset](#)

### Time

#### ☒ Manually Set Date and Time

2000 / 01 / 01 00 : 53

#### ☐ Automatically Get Date and Time

Time Zone: UTC+00:00 England

☐ User defined NTP Server: 0 . 0 . 0 . 0[Apply](#)[Cancel](#)

- **Manually Set Date and Time:** Specify the date and time
- **Automatically Get Date and Time:** Select the time zone from the drop down list and then specify the IP address of the NTP server.
- Click on the **Apply** button to save the changes.

## 4.5.7 Log

- Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

## Log

[Home](#)[Reset](#)

### Syslog

Syslog

Disable

Log Server IP Address

0 . 0 . 0 . 0

### Local log

Local Log

Disable

[Apply](#)[Cancel](#)

- **Syslog:** Choose to enable or disable the system log.
- **Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- **Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

## 4.5.8 Diagnostics

- Click on the **Diagnostics** link under the **Management** menu. In this page, user can let unit to ping other network equipment. And user also can monitor a route from unit to your target.

## Diagnostics

[Home](#)[Reset](#)

### Ping Test Parameters

Target IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Ping Size	<input type="text" value="64"/> Bytes
Number of Pings	<input type="text" value="4"/>

[Start Ping](#)

### Traceroute Test Parameters

Traceroute target	<input type="text"/>
-------------------	----------------------

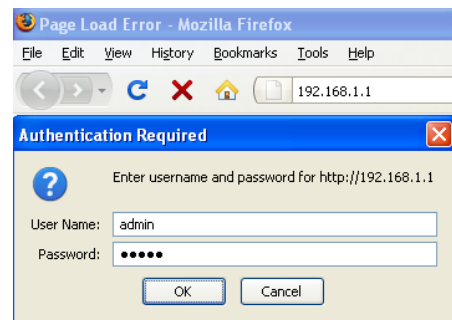
[Start Traceroute](#)

- **Ping Test Parameters** : User can input Target IP, Ping Size and Ping Quantity of other network device which connected you want. And then you can find the ping condition after click Start Ping.
- **Traceroute Test Parameters**: This function help user to monitor a network trace. User can input IP or domain name on Traceroute target.

## 5 Client Bridge Operating Mode

### 5.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.
- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:
  1. **Status:** Displays the overall status, connection status, and system log.
  2. **System:** This menu includes the system properties, IP and Spanning Tree settings.
  3. **Wireless:** This menu includes network, security and advanced settings.
  4. **Management:** This menu includes the admin setup, SNMP, firmware upgrade, time settings, diagnostics and save/restore backup.



**Wireless Access Point / Client Bridge**

**Client Bridge**

---

**Status**

- Main
- Connection Status
- System Log

**System**

- System Properties
- IP Settings
- Spanning Tree Settings

**Wireless**

- Wireless Network
- Wireless Security
- Wireless Advanced Settings

**Management**

- Administration
- SNMP Settings
- Backup/Restore Settings
- Firmware Upgrade
- Time Settings
- Log
- Diagnostics

[Home](#) [Reset](#)

---

**Main**

**System Information**

Device Name	Access Point
Ethernet MAC Address	00:02:6f:57:87:0a
Wireless MAC Address	00:02:6f:57:87:0b
Country	N/A
Current Time	Sat Jan 1 00:09:06 UTC 2000
Firmware Version	1.0.39

**LAN Settings**

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

**Current Wireless Settings**

Operation Mode	Client Bridge
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.417GHz (channel 02)
Wireless Network Name (SSID)	EnGenius
Security	Disabled
Spanning Tree Protocol	Disabled
Distance	1 Km

[Refresh](#)

## 5.2 Status

### Status

- Main
- Connection Status
- System Log

- Click on the **Status** link on the navigation drop-down menu. You will then see three options: Main, Connection Status, and System Log. Each option is described in detail below.

### 5.2.1 Main

- Click on the **Main** link under the **Status** drop-down menu. The status that is displayed corresponds with the operating mode that is selected. Information such as device name, firmware version, MAC address, country and current time are displayed in the 'System Information' section. IP address, subnet mask, default gateway and DHCP client are displayed in the 'LAN Settings' section. In the 'Current Wireless Settings' section, the operation mode, wireless mode, channel/frequency, SSID, security and distance are displayed.

#### Main

[Home](#)[Reset](#)

##### System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:57:87:0a
Wireless MAC Address	00:02:6f:57:87:0b
Country	N/A
Current Time	Sat Jan 1 00:06:37 UTC 2000
Firmware Version	1.0.39

##### LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

##### Current Wireless Settings

Operation Mode	Client Bridge
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.452GHz (channel 09)
Wireless Network Name (SSID)	EnGenius
Security	Disabled
Spanning Tree Protocol	Disabled
Distance	1 Km

[Refresh](#)

### 5.2.2 Connection Status

- Click on the **Connection Status** link under the **Status** drop-down menu. This page displays the current status of the network, including network type, SSID, BSSID, connection status, wireless mode, current channel, security, data rate, noise level and signal strength.

### Connection Status

[Home](#)[Reset](#)

Network Type	Client Bridge
SSID	EnGenius
BSSID	N/A
Connection Status	N/A
Wireless Mode	N/A
Current Channel	N/A
Security	N/A
Tx Data Rate(Mbps)	N/A
Current noise level	N/A
Signal strength	N/A

[Refresh](#)

### 5.2.3 System Log

- Click on the **System Log** link under the **Status** drop-down menu. The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.

### System Log

[Home](#)[Reset](#)Show log type 

Local Log is disabled.

[Refresh](#)[Clear](#)

## 5.3 System

### System

- System Properties
- IP Settings
- Spanning Tree Settings

- Click on the **System** link on the navigation drop-down menu. You will then see three options: System Properties, IP Settings, and Spanning Tree Settings. Each option is described in detail below.

### 5.3.1 System Properties

- Click on the **System Properties** link under the **System** drop-down menu. This page allows you to switch the operating mode of the device, as well as specify a name and select the operating region.

#### System Properties

[Home](#)[Reset](#)

Device Name	<input type="text" value="Access Point"/> ( 1 to 32 characters )
Country/Region	<input type="text" value="Please Select a Country Code"/>
Operation Mode	<input type="radio"/> Access Point <input checked="" type="radio"/> Client Bridge <input type="radio"/> WDS Bridge <input type="radio"/> Client Router

[Apply](#)[Cancel](#)

- **Device Name:** Specify a name for the device (this is not the SSID),
- **Country/Region:** Select a country from the drop-down list.
- **Operating Mode:** Select an operating mode. Configuration for each operating mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

### 5.3.2 IP Settings

- Click on the **IP Settings** link under the **System** drop-down menu. This page allows you to configure the device with a static IP address or a DHCP client.

#### IP Settings

[Home](#)[Reset](#)

IP Network Setting	<input type="radio"/> Obtain an IP address automatically (DHCP) <input checked="" type="radio"/> Specify an IP address
IP Address	<input type="text" value="19"/> . <input type="text" value="16"/> . <input type="text" value="1"/> . <input type="text" value="1"/>
IP Subnet Mask	<input type="text" value="25"/> . <input type="text" value="25"/> . <input type="text" value="25"/> . <input type="text" value="0"/>
Default Gateway	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

[Apply](#)[Cancel](#)

- **IP Network Setting:** Select **Obtain an IP address automatically (DHCP)** radio button if the Access Point is connected to a DHCP server. This will allow the Access Point to pass IP addresses to the clients associated with it. You may select **Specify an IP Address** radio button if you would like the



device to use a static IP address. In this case, you would be required to specify an IP address, subnet mask, and default gateway IP address.

- **IP Address:** Specify an IP address
- **IP Subnet Mask:** Specify the subnet mask for the IP address
- **Default Gateway:** Specify the IP address of the default gateway.
- Click on the **Apply** button to save the changes.

### 5.3.3 Spanning Tree Settings

- Click on the **Spanning Tree** link under the **System** drop-down menu Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

**Spanning Tree Settings**

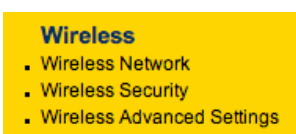
HomeReset

Spanning Tree Status	<input type="radio"/> On <input checked="" type="radio"/> Off
Bridge Hello Time	1 seconds (1-10)
Bridge Max Age	20 seconds (6-40)
Bridge Forward Delay	4 seconds (4-30)
Priority	32768 seconds (0-65535)

ApplyCancel

- **Spanning Tree Status:** Choose to enable or disable the spanning tree feature.
- **Bridge Hello Time:** Specify the number of seconds for the hello time.
- **Bridge Max Age:** Specify the number of seconds for the max age.
- **Bridge Forward Delay:** Specify the number of seconds for the bridge forward delay.
- **Priority:** Specify the number of seconds for the priority.
- Click on the **Apply** button to save the changes.

## 5.4 Wireless



- Click on the **Wireless** link on the navigation drop-down menu. You will then see three options: wireless network, wireless security, and wireless advanced settings. Each option is described below.

### 5.4.1 Wireless Network

- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.

## Wireless Network

Home

Reset

Wireless Mode	802.11b/g Mixed (2GHz/54Mbps)
SSID	Specify the static SSID : <input type="text" value="EnGenius"/> ( 1 to 32 characters ) Or press the button to search for any available WLAN Service. <input type="button" value="Site Survey"/>
Prefer BSSID	<input type="checkbox"/> <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/> : <input type="checkbox"/>
WDS Client	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Apply

Cancel

- **Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **B**, **G**, or **B/G-mixed**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.
- **SSID:** The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters. You may specify an SSID or select one from the **Site Survey**.
- **Site Survey:** Click on the **Site Survey** button in order to scan the 2.4GHz frequency for devices that broadcast their SSID. Click on the **BSSID** link to connect to the Access Point. Click on the **Refresh** button to re-scan the frequency.

## Site Survey

## 2.4GHz Site Survey

☒ Infrastructure ☐ Ad\_hoc

BSSID	SSID	Channel	Signal	Type	Security	Network Mode
00:e0:4c:81:86:21	DinoNet	1	-86 dBm	B	WEP	<input checked="" type="radio"/>
00:13:d7:7c:6f:43	SMC	6	-105 dBm	G	NONE	<input checked="" type="radio"/>

Refresh

## 5.4.2 Wireless Security

- You can change the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

## Wireless Security

Home

Reset

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	Disabled
---------------	----------

Apply

Cancel

## Wireless Security : WEP

- **Security Mode:** Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.

### Wireless Security

[Home](#)[Reset](#)

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	40/64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	
Key2	
Key3	
Key4	

[Apply](#)[Cancel](#)

- **Authentication Type:** Select an authentication method. Options available are **Open Key**, **Shared Key**. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the Access Point. The device requesting authentication encrypts the challenge text and sends it back to the Access Point. If the challenge text is encrypted correctly, the Access Point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- **Input Type:** Select Hex or ASCII from the drop-down list
- **Key Length:** Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F and a through f.
- **Default Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Key 1-4:** You may enter four different WEP keys.
- Click on the **Apply** button to save the changes.

### Wireless Security : WPA2-PSK

- **Security Mode:** Select **WPA2-PSK** from the drop-down list if your wireless network uses WPA pre-shared key.

## Wireless Security

[Home](#)[Reset](#)

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA2-PSK
Encryption	TKIP
Passphrase	<input type="text"/> (8 to 63 characters) or (64 Hexadecimal characters)

[Apply](#)[Cancel](#)

- **Encryption:** Select **TKIP** or **AES** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- **Passphrase:** Specify a passphrase that is shared amongst the Access Points and clients.
- Click on the **Apply** button to save the changes.

### Wireless Security : WPA-PSK

- **Security Mode:** Select **WPA-PSK** from the drop-down list if your wireless network uses WPA pre-shared key.

## Wireless Security

[Home](#)[Reset](#)

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA-PSK
Encryption	TKIP
Passphrase	<input type="text"/> (8 to 63 characters) or (64 Hexadecimal characters)

[Apply](#)[Cancel](#)

- **Encryption:** Select **TKIP** or **AES** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- **Passphrase:** Specify a passphrase that is shared amongst the Access Points and clients. Click on the **Apply** button to save the changes.

### 5.4.3 Wireless Advanced Settings

- Click on the **Wireless Advanced Settings** link. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, fragmentation threshold, RTS threshold, protection mode and distance.

## Wireless Advanced Settings

[Home](#)
[Reset](#)

Data Rate	Auto
Transmit Power	20 dBm
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	1 km

[Apply](#)
[Cancel](#)

- **Data Rate:** If you would like to force a data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Transmit Power:** You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **Fragment:** Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Protection Mode:** If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **Distance (1-30km):** Specify a distance between 1 and 30Km.
- Click on the **Apply** button to save the changes.

## 5.5 Management

### Management

- Administration
- SNMP Settings
- Backup/Restore Settings
- Firmware Upgrade
- Time Settings
- Log
- Diagnostics

- Click on the **Management** link on the navigation drop-down menu. You will then see six options: administration, SNMP settings, backup/restore settings, firmware upgrade, time settings, and log. Each option is described below.

### 5.5.1 Administration

- Click on the **Administration** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.

## Administration

[Home](#)[Reset](#)

### Administrator

Name	<input type="text" value="admin"/>
Password	<input type="password" value="....."/>
Confirm Password	<input type="password" value="....."/>

[Apply](#)[Cancel](#)

- **Name:** Specify a user name into the first field.
- **Password:** Specify a password into this field and then re-type the password into the **Confirm Password** field.
- Click on the **Apply** button to save the changes.

## 5.5.2 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases.

## SNMP Settings

[Home](#)[Reset](#)

SNMP Enable/Disable	<input checked="" type="radio"/> <b>Enable</b> <input type="radio"/> <b>Disable</b>
Contact	<input type="text"/>
Location	<input type="text"/>
Community Name (Read Only)	<input type="text" value="public"/>
Community Name (Read/Write)	<input type="text" value="private"/>
Trap Destination IP Address	<input type="text" value="0 . 0 . 0 . 0"/>
Trap Destination Community Name	<input type="text" value="public"/>

[Apply](#)[Cancel](#)

- **SNMP Enable/Disable:** Choose to **enable** or **disable** the SNMP feature.
- **Contact:** Specify the contact details of the device.
- **Location:** Specify the location of the device.
- **Read-Only Community Name:** Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name:** Specify the password for access to the SNMP community with read/write access.
- **Send SNMP Trap:** Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Community Name:** Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

### 5.5.3 Backup/Restore settings, Reset to factory default settings

- Click on the **Backup/Restore Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.

**Backup/Restore Settings**

HomeReset

Save A Copy of Current Settings	Backup
Restore Saved Settings from A File	選擇檔案 尚未選取檔案Restore
Revert to Factory Default Settings	Factory Default

- Save a copy of the current settings:** Click on the Backup button to save the current configuration.
- Restore saved settings from a file:** Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- Revert to factory default settings:** Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: 192.168.1.1

#### System Rebooting...

Rebooting, Please wait... 88

[Click here when AP is ready](#)

### 5.5.4 Firmware Upgrade

- Click on the **Upgrade Firmware** link under the **Management** menu. This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.

**Firmware Upgrade**

HomeReset

Current firmware version: 1.0.39

Locate and select the upgrade file from your hard disk:

選擇檔案 尚未選取檔案

Upgrade

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** button.  
**Note:** The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

### 5.5.5 Time Settings

- Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.

**Time Settings** Home Reset

Time

☒ **Manually Set Date and Time**

2000 / 01 / 01 01 : 03

☐ **Automatically Get Date and Time**

Time Zone: UTC+00:00 England

☐ **User defined NTP Server:** 0 . 0 . 0 . 0

Apply Cancel

- Manually Set Date and Time:** Specify the date and time
- Automatically Get Date and Time:** Select the time zone from the drop down list and then specify the IP address of the NTP server.
- Click on the **Apply** button to save the changes.

### 5.5.6 Log

- Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

**Log** Home Reset

Syslog

Syslog Disable

Log Server IP Address 0 . 0 . 0 . 0

Local log

Local Log Disable

Apply Cancel

- Syslog:** Choose to enable or disable the system log.
- Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

### 5.5.7 Diagnostics

- Click on the **Diagnostics** link under the **Management** menu. In this page, user can let unit to ping other network equipment. And user also can monitor a route from unit to your target.



## Diagnostics

[Home](#)[Reset](#)

### Ping Test Parameters

Target IP	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
Ping Size	<input type="text" value="64"/> Bytes
Number of Pings	<input type="text" value="4"/>

[Start Ping](#)

### Traceroute Test Parameters

Traceroute target	<input type="text"/>
-------------------	----------------------

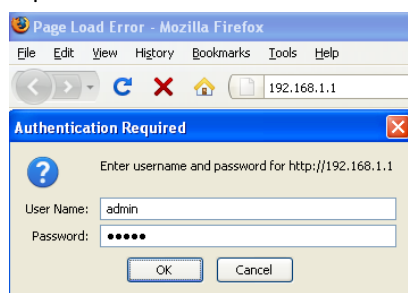
[Start Traceroute](#)

- **Ping Test Parameters** : User can input Target IP, Ping Size and Ping Quantity of other network device which connected you want. And then you can find the ping condition after click Start Ping.
- **Traceroute Test Parameters**: This function help user to monitor a network trace. User can input IP or domain name on Traceroute target.

## 6 WDS Bridge Operating Mode

### 6.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.
- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:
  1. **Status:** Displays the overall status, WDS link status and system log.
  2. **System:** This menu includes the system properties, IP and Spanning Tree settings.
  3. **Wireless:** This menu includes network setting, WDS link setting, WDS security and advanced setting.
  4. **Management:** This menu includes the admin setup, SNMP, firmware upgrade, time setting, diagnostics and save/restore backup.



EnGenius | Wireless Access Point / Client Bridge

WDS Bridge

**Status**

- Main
- WDS Link Status
- System Log

**System**

- System Properties
- IP Settings
- Spanning Tree Settings

**Wireless**

- Wireless Network
- WDS Link Settings
- WDS Security
- Wireless Advanced Settings

**Management**

- Administration
- SNMP Settings
- Backup/Restore Settings
- Firmware Upgrade
- Time Settings
- Log
- Diagnostics

[Home](#)   [Reset](#)

**Main**

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:57:87:0a
Wireless MAC Address	00:02:6f:57:87:0b
Country	N/A
Current Time	Sat Jan 1 00:11:37 UTC 2000
Firmware Version	1.0.39

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

Current Wireless Settings

Operation Mode	WDS Bridge
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Spanning Tree Protocol	Disabled
Distance	1 Km

[Refresh](#)

## 6.2 Status

### Status

- Main
- WDS Link Status
- System Log

- Click on the **Status** link on the navigation drop-down menu. You will then see three options: Main, WDS Link Status, and System Log. Each option is described in detail below.

### 6.2.1 Main

- Click on the **Main** link under the **Status** drop-down menu. The status that is displayed corresponds with the operating mode that is selected. Information such as Device Name, Ethernet MAC Address, Wireless MAC Address, Country, Current Time and Firmware are displayed in the 'System Information' section. IP address, Subnet Mask, Default Gateway and DHCP Client are displayed in the 'LAN Settings' section. In the 'Current Wireless Settings' section, the Operation Mode, Wireless Mode, Channel/Frequency, Spanning Tree Protocol and Distance are displayed.

#### Main

[Home](#)[Reset](#)

##### System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:57:87:0a
Wireless MAC Address	00:02:6f:57:87:0b
Country	N/A
Current Time	Sat Jan 1 00:07:33 UTC 2000
Firmware Version	1.0.39

##### LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Client	Disabled

##### Current Wireless Settings

Operation Mode	WDS Bridge
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.412GHz (channel 01)
Spanning Tree Protocol	Disabled
Distance	1 Km

[Refresh](#)

### 6.2.2 WDS Link Status

- Click on the **WDS Link Status** link under the **Status** drop-down menu. This page displays the current status of the WDS Link, including Station ID, MAC address, Status, RSSI(Received Signal Strength Indicator).

**WDS Link Status**

HomeReset

Station ID	MAC Address	Status	RSSI (dBm)
<div>Refresh</div>			

### 6.2.3 System Log

- Click on the **System Log** link under the **Status** drop-down menu. The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.

**System Log**

HomeReset

Show log type 

All

Local Log is disabled.

Refresh

Clear

## 6.3 System

### System

- System Properties
- IP Settings
- Spanning Tree Settings

- Click on the **System** link on the navigation drop-down menu. You will then see System Properties, IP Settings and Spanning Tree Settings.

### 6.3.1 System Properties

- Click on the **System Properties** link under the **System** drop-down menu. This page allows you to switch the operating mode of the device, as well as specify a name and select the operating region.

System Properties		Home	Reset
Device Name	<input type="text" value="Access Point"/> ( 1 to 32 characters )		
Country/Region	<input type="text" value="Please Select a Country Code"/>		
Operation Mode	<input type="radio"/> Access Point <input type="radio"/> Client Bridge <input checked="" type="radio"/> WDS Bridge <input type="radio"/> Client Router		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- **Device Name:** Specify a name for the device (this is not the SSID),
- **Country/Region:** Select a country from the drop-down list.
- **Operating Mode:** Select an operating mode. Configuration for each operating mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

### 6.3.2 IP Settings

Click on the **IP Settings** link under the **System** drop-down menu. This page allows you to configure the device with a static IP address or a DHCP client.

IP Settings		Home	Reset
IP Network Setting	<input type="radio"/> Obtain an IP address automatically (DHCP) <input checked="" type="radio"/> Specify an IP address		
IP Address	<input type="text" value="19"/> . <input type="text" value="16"/> . <input type="text" value="1"/> . <input type="text" value="1"/>		
IP Subnet Mask	<input type="text" value="25"/> . <input type="text" value="25"/> . <input type="text" value="25"/> . <input type="text" value="0"/>		
Default Gateway	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

- **IP Network Setting:** Select **Obtain an IP address automatically (DHCP)** radio button if the Access Point is connected to a DHCP server. This will allow the Access Point to pass IP addresses to the clients associated with it. You may select **Specify an IP Address** radio button if you would like the device to use a static IP address. In this case, you would be required to specify an IP address, subnet mask, and default gateway IP address.
- **IP Address:** Specify an IP address
- **IP Subnet Mask:** Specify the subnet mask for the IP address
- **Default Gateway:** Specify the IP address of the default gateway.
- Click on the **Apply** button to save the changes.

### 6.3.3 Spanning Tree Settings

Click on the **Spanning Tree** link under the **System** drop-down menu Spanning-Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network.

Spanning Tree Settings		Home	Reset
Spanning Tree Status	<input type="radio"/> On <input checked="" type="radio"/> Off		
Bridge Hello Time	1	seconds (1-10)	
Bridge Max Age	20	seconds (6-40)	
Bridge Forward Delay	4	seconds (4-30)	
Priority	32768	seconds (0-65535)	

- **Spanning Tree Status:** Choose to enable or disable the spanning tree feature.
- **Bridge Hello Time:** Specify the number of seconds for the hello time.
- **Bridge Max Age:** Specify the number of seconds for the max age.
- **Bridge Forward Delay:** Specify the number of seconds for the bridge forward delay.
- **Priority:** Specify the number of seconds for the priority.
- Click on the **Apply** button to save the changes.

## 6.4 Wireless

### Wireless

- Wireless Network
- WDS Link Settings
- WDS Security
- Wireless Advanced Settings

- Click on the **Wireless** link on the navigation drop-down menu. You will then see four options: Wireless Network, WDS Link Settings, WDS Security and Wireless Advanced Settings. Each section is described in detail below.

### 6.4.1 Wireless Network

- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.

Home
Reset

**Wireless Network**

Wireless Mode

802.11b/g Mixed (2GHz/54Mbps)

Channel / Frequency

Ch1-2.412GHz

Apply
Cancel

- Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **B**, **G** or **B/G-mixed**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.
- Channel/Frequency:** Select a channel from the drop-down list. The channels available are based on the country's regulation.

### 6.4.2 WDS Link Settings

- Click on the **WDS Link Settings** link under the **Wireless** drop-down menu. This page allows you to setting your WDS device link up to 16 units.

Home
Reset

**WDS Link Settings**

ID	MAC Address	Mode
1	<input type="text" value=" : : : : :"/>	Disable
2	<input type="text" value=" : : : : :"/>	Disable
3	<input type="text" value=" : : : : :"/>	Disable
4	<input type="text" value=" : : : : :"/>	Disable
5	<input type="text" value=" : : : : :"/>	Disable
6	<input type="text" value=" : : : : :"/>	Disable
7	<input type="text" value=" : : : : :"/>	Disable
8	<input type="text" value=" : : : : :"/>	Disable
9	<input type="text" value=" : : : : :"/>	Disable
10	<input type="text" value=" : : : : :"/>	Disable
11	<input type="text" value=" : : : : :"/>	Disable
12	<input type="text" value=" : : : : :"/>	Disable
13	<input type="text" value=" : : : : :"/>	Disable
14	<input type="text" value=" : : : : :"/>	Disable
15	<input type="text" value=" : : : : :"/>	Disable
16	<input type="text" value=" : : : : :"/>	Disable

Apply
Cancel

- **MAC Address:** you can input the MAC address of WDS device, which you want to link.
- **Mode:** Enable to connect, and Disable to disconnect.
- Click on the **Apply** button to save the changes.

### 6.4.3 WDS Security

The screenshot shows the 'WDS Security' configuration page. At the top right are 'Home' and 'Reset' buttons. The 'Security' dropdown menu is set to 'None'. The 'WEP Key' field is empty, and the key format dropdown is set to '40/ 64-bit(10 hex digits)'. At the bottom are 'Apply' and 'Cancel' buttons.

- **Security Mode:** Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.

This screenshot shows the 'WDS Security' page with 'Security' set to 'WEP'. The 'WEP Key' field is empty. A dropdown menu for the key format is open, showing three options: '40/ 64-bit(10 hex digits)' (selected with a checkmark), '104/128-bit(26 hex digits)', and '128/152-bit(32 hex digits)'. 'Apply' and 'Cancel' buttons are at the bottom.

- **WEP Key:** Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters and 152-bits keys require 32 characters. A hex key is defined as a number between 0 through 9 and letter between A through F and a through f.
- Click on the **Apply** button to save the changes.

### 6.4.4 Wireless Advanced Settings

Click on the **Wireless Advanced Settings** link. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, fragmentation threshold, RTS threshold, protection mode and distance.



### Wireless Advanced Settings

[Home](#)[Reset](#)

Data Rate	Auto
Transmit Power	20 dBm
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	1 km

[Apply](#)[Cancel](#)

- **Data Rate:** If you would like to force a data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Transmit Power:** You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **Fragment Length:** Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS/CTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Protection Mode:** If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **WMM:** Enable wireless Quality of Service
- **Distance (1-30km):** Specify a distance between 1 and 30Km.
- Click on the **Apply** button to save the changes.

## 6.5 Management

### Management

- Administration
- SNMP Settings
- Backup/Restore Settings
- Firmware Upgrade
- Time Settings
- Log
- Diagnostics

- Click on the **Management** link on the navigation drop-down menu. You will see seven options: Administration, SNMP Settings, Backup/Restore Settings, Firmware Upgrade, Time Settings, Log and Diagnostics. Each option is described below.

### 6.5.1 Administration

- Click on the **Administration** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.

**Administration**

HomeReset

Administrator

Name	admin
Password	.....
Confirm Password	.....

ApplyCancel

- Name:** Specify a user name into the first field.
- Password:** Specify a password into this field and then re-type the password into the **Confirm Password** field.
- Click on the **Apply** button to save the changes.

### 6.5.2 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases. .

**SNMP Settings**

HomeReset

SNMP Enable/Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	
Location	
Community Name (Read Only)	public
Community Name (Read/Write)	private
Trap Destination IP Address	0 . 0 . 0 . 0
Trap Destination Community Name	public

ApplyCancel

- SNMP Enable/Disable:** Choose to **enable** or **disable** the SNMP feature.
- Contact:** Specify the contact details of the device.
- Location:** Specify the location of the device.

- **Read-Only Community Name:** Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name:** Specify the password for access to the SNMP community with read/write access.
- **Trap Destination IP Address:** Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Destination Community Name:** Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

### 6.5.3 Backup/Restore settings, Reset to factory default settings

- Click on the **Backup/Restore Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.

**Backup/Restore Settings**

HomeReset

Save A Copy of Current Settings	Backup
Restore Saved Settings from A File	選擇檔案 尚未選取檔案Restore
Revert to Factory Default Settings	Factory Default

- **Save a copy of the current settings:** Click on the Backup button to save the current configuration.
- **Restore saved settings from a file:** Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings:** Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: 192.168.1.1

System Rebooting...

Rebooting, Please wait... 

[Click here when AP is ready](#)

### 6.5.4 Firmware Upgrade

- Click on the **Upgrade Firmware** link under the **Management** menu. This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.

## Firmware Upgrade

[Home](#)[Reset](#)

Current firmware version: 1.0.39

Locate and select the upgrade file from your hard disk:

[選擇檔案](#) 尚未選取檔案[Upgrade](#)

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** button.

**Note:** The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

### 6.5.5 Time Settings

- Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.

## Time Settings

[Home](#)[Reset](#)

Time

☒ Manually Set Date and Time

2000 / 01 / 01 00 : 36

☐ Automatically Get Date and Time

Time Zone: UTC+00:00 England

☐ User defined NTP Server: 0 . 0 . 0 . 0[Apply](#)[Cancel](#)

- Manually Set Date and Time:** Specify the date and time
- Automatically Get Date and Time:** Select the time zone from the drop down list and then specify the IP address of the NTP server.
- Click on the **Apply** button to save the changes.

### 6.5.6 Log

- Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

**Log**

HomeReset

---

**Syslog**

Syslog	Disable
Log Server IP Address	0 . 0 . 0 . 0

**Local log**

Local Log	Disable
-----------	---------

ApplyCancel

- **Syslog:** Choose to enable or disable the system log.
- **Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- **Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

### 6.5.7 Diagnostics

- Click on the **Diagnostics** link under the **Management** menu. In this page, user can let unit to ping other network equipment. And user also can monitor a route from unit to your target.

**Diagnostics**

HomeReset

---

**Ping Test Parameters**

Target IP	
Ping Size	64 Bytes
Number of Pings	4

Start Ping

**Traceroute Test Parameters**

Traceroute target	
-------------------	--

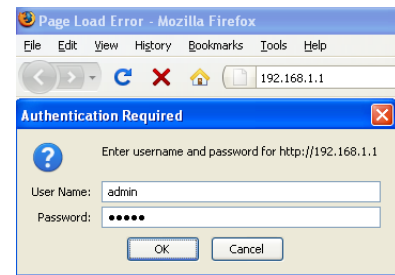
Start Traceroute

- **Ping Test Parameters :** User can input Target IP, Ping Size and Ping Quantity of other network device which connected you want. And then you can find the ping condition after click **Start Ping**.
- **Traceroute Test Parameters:** This function help user to monitor a network trace. User can input IP or domain name on Traceroute target.

## 7 Client Router Operating Mode

### 7.1 Logging In

- To configure the device through the web-browser, enter the IP address of the device (default: **192.168.1.1**) into the address bar of the web-browser and press **Enter**.
- Make sure that the device and your computers are configured on the same subnet. Refer to **Chapter 2** in order to configure the IP address of your computer.
- After connecting to the IP address, the web-browser will display the login page.
- Specify **admin** for both the user name and password.
- After logging in you will graphical user interface (GUI) of the device. The navigation drop-down menu on left is divided into four sections:
  1. **Status**: Displays the overall status, DHCP client table, connection status and system log.
  2. **System**: This menu includes the system properties.
  3. **Router**: This includes WAN, LAN, and VPN settings.
  4. **Wireless**: This menu includes wireless network, security and advanced settings.
  5. **Management**: This menu includes the admin setup, SNMP settings, firmware upgrade, save/restore backup, time setting and diagnostics.



EnGenius®

Wireless Access Point / Client Bridge

Client Router

Status

- Main
- DHCP Client Table
- Connection Status
- System Log

System

- System Properties

Router

- WAN Settings
- LAN Settings
- VPN Pass Through

Wireless

- Wireless Network
- Wireless Security
- Wireless Advanced Settings

Management

- Administration
- SNMP Settings
- Backup/Restore Settings
- Firmware Upgrade
- Time Settings
- Log
- Diagnostics

Main

HomeReset

System Information

Device Name	Access Point
Ethernet MAC Address	00:02:6f:57:87:0a
Wireless MAC Address	00:02:6f:57:87:0b
Country	N/A
Current Time	Sat Jan 1 00:13:37 UTC 2000
Firmware Version	1.0.39

LAN Settings

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Enabled

WAN Settings

MAC Address	00:02:6f:57:87:0b
Connection Type	Static IP
Interface	down
IP Address	
IP Subnet Mask	0.0.0.0

Current Wireless Settings

Operation Mode	Client Router
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.442GHz (channel 07)
Wireless Network Name (SSID)	EnGenius
Security	Disabled

### 7.2 Status

**Status**

- Main
- DHCP Client Table
- Connection Status
- System Log

- Click on the **Status** link on the navigation drop-down menu. You will then see four options: Main, DHCP Client Table, Connection Status and System Log. Each option is described in detail below.

**7.2.1 Main**

- Click on the **Main** link under the **Status** drop-down menu. The status that is displayed corresponds with the operating mode that is selected. Information such as Device Name, MAC Address, Country, Current and Firmware Version are displayed in the 'System Information' section. IP Address, Subnet Mask, Default Gateway and DHCP Server condition are displayed in the 'LAN Settings' section. In the 'WAN Settings', MAC Address, Connection Type, Interface and IP Address/Subnet Mask are displayed. The 'Current Wireless Settings' section displays Operation Mode, Wireless Mode, Channel/Frequency, SSID, Security and Distance control.

**Main**[Home](#)[Reset](#)**System Information**

Device Name	Access Point
Ethernet MAC Address	00:02:6f:57:87:0a
Wireless MAC Address	00:02:6f:57:87:0b
Country	N/A
Current Time	Sat Jan 1 00:01:56 UTC 2000
Firmware Version	1.0.39

**LAN Settings**

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	0.0.0.0
DHCP Server	Enabled

**WAN Settings**

MAC Address	00:02:6f:57:87:0b
Connection Type	Static IP
Interface	down
IP Address	
IP Subnet Mask	0.0.0.0

**Current Wireless Settings**

Operation Mode	Client Router
Wireless Mode	IEEE 802.11b/g Mixed
Channel/Frequency	2.427GHz (channel 04)
Wireless Network Name (SSID)	EnGenius
Security	Disabled
Distance	1 Km

[Refresh](#)

### 7.2.2 DHCP Client Table

- Click on the **DHCP Client Table** link under the **Status** drop-down menu. This page displays the current status of all DHCP clients, including IP and expires information.

#### DHCP Client List

[Home](#)[Reset](#)

MAC addr	IP	Expires
<a href="#">Refresh</a>		

### 7.2.3 Connection Status

Click on the **Connection Status** link under the **Status** drop-down menu. This page displays the current status of the network, including network type, SSID, BSSID, connection status, wireless mode, current channel, security, data rate, noise level and signal strength.

#### Connection Status

[Home](#)[Reset](#)

##### Wireless

Network Type	Client Router
SSID	EnGenius
BSSID	N/A
Connection Status	N/A
Wireless Mode	N/A
Current Channel	N/A
Security	N/A
Tx Data Rate(Mbps)	N/A
Current noise level	N/A
Signal strength	N/A

##### WAN

MAC Address	00:02:6f:57:87:0b
Connection Type	Static IP
Interface	down
IP Address	
IP Subnet Mask	0.0.0.0

[Refresh](#)



### 7.2.4 System Log

Click on the **System Log** link under the **Status** drop-down menu. The device automatically logs (records) events of possible interest in its internal memory. If there is not enough internal memory for all events, logs of older events are deleted, but logs of the latest events are retained.

**System Log**

HomeReset

Show log typeAll

Local Log is disabled.

RefreshClear

## 7.3 System

### System

- System Properties

- Click on the **System** link on the navigation drop-down menu. You will then see System Properties setting, which is described below.

### 7.3.1 System Properties

- Click on the **System Properties** link under the **System** drop-down menu. This page allows you to switch the operating mode of the device, as well as specify a name and select the operating region.

#### System Properties

[Home](#)[Reset](#)

Device Name	<input type="text" value="Access Point"/> ( 1 to 32 characters )
Country/Region	<input type="text" value="Please Select a Country Code"/>
Operation Mode	<input type="radio"/> Access Point <input type="radio"/> Client Bridge <input type="radio"/> WDS Bridge <input checked="" type="radio"/> Client Router

[Apply](#)[Cancel](#)

- Device Name:** Specify a name for the device (this is not the SSID),
- Country/Region:** Select a country from the drop-down list.
- Operating Mode:** Select operating mode. Configuration for each operating mode is described in their respective chapters.
- Click on the **Apply** button to save the changes.

## 7.4 Router

### Router

- WAN Settings
- LAN Settings
- VPN Pass Through

- Click on the **Router** link on the navigation drop-down menu. You will then see three options: WAN settings, LAN settings, and VPN Pass Through. Each section is described in detail below.

### 7.4.1 WAN Settings

- Click on the **WAN Settings** link under the **Router** drop-down menu. This page allows you to configure the WAN interface as DHCP, Static IP, PPPoE or PPTP.

### 7.4.1.1 WAN - DHCP

- The WAN interface can be configured as a DHCP Client in which the ISP provides the IP address to the device. This is also known as Dynamic IP.

**WAN Settings** Home Reset

Internet Connection Type: DHCP

**Options**

Account Name (if required)	<input type="text" value="none"/>
Domain Name (if required)	<input type="text" value="none"/>
MTU	<span>Auto</span> <span>1500</span>

**Domain Name Server (DNS) Address**

☒ Get Automatically From ISP

☐ Use These DNS Servers

Primary DNS	<input type="text" value="0 . 0 . 0 . 0"/>
Secondary DNS	<input type="text" value="0 . 0 . 0 . 0"/>

Apply Cancel

- **Internet Connection Type:** Select the **DHCP** from the drop-down list.
- **Account Name:** Specify an account name if your ISP has provided you with one.
- **Domain Name:** Specify a domain name if the ISP has provided you with one.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **Domain Name Service:** Select **Get Automatically from ISP** if the ISP will provide the DNS address, if not, select **Use these DNS servers** and specify the primary and secondary DNS server IP address.
- Click on the **Apply** button to save the changes.

### 7.4.1.2 WAN – Static IP

- The WAN interface can be configured as Static IP address. In this type of connection, your ISP provides you with a dedicated IP address (which does not change as DHCP).

**WAN Settings**

Home

Reset

Internet Connection Type	Static IP
Options	
Account Name (if required)	none
Domain Name (if required)	none
MTU	Auto 1500
Internet IP Address	
IP Address	10 . 1 . 1 . 10
IP Subnet Mask	255 . 255 . 0 . 0
Gateway IP Address	10 . 1 . 1 . 15
Domain Name Server (DNS) Address	
Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

- **Internet Connection Type:** Select the **Static IP** from the drop-down list.
- **Account Name:** Specify an account name if your ISP has provided you with one.
- **Domain Name:** Specify a domain name if the ISP has provided you with one.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **IP Address:** Specify the IP address for this device, which is assigned by your ISP.
- **Subnet Mask:** Specify the subnet mask for this IP address, which is assigned by your ISP.
- **Gateway IP Address:** Specify the IP address of the default gateway, which is assigned by your ISP.
- **Domain Name Service:** Specify the primary and secondary DNS server IP address.
- Click on the **Apply** button to save the changes.

**7.4.1.3 WAN – PPPoE**

- The WAN interface can be configured as PPPoE. This type of connection is usually used for a DSL service and requires a username and password to connect.

**WAN Settings**

Home

Reset

Internet Connection Type

PPPoE

## Options

MTU

Auto

1492

## PPPoE Options

Login

Password

Service Name (if required)

☐ Connect on Demand: Max Idle Time 1 Minutes☒ Keep Alive: Redial Period 30 Seconds

## Domain Name Server (DNS) Address

☒ Get Automatically From ISP☐ Use These DNS Servers

Primary DNS

0 . 0 . 0 . 0

Secondary DNS

0 . 0 . 0 . 0

Apply

Cancel

- **Internet Connection Type:** Select **PPPoE** from the drop-down list.
- **MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- **Login:** Specify the user name which is provided by your ISP.
- **Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- **Service Name:** Specify the name of the ISP.
- **Type:** Select a reconnection type: **Keep Alive** (A connection to the Internet is always maintained), **Connect on Demand:** You have to open up the Web-based management interface and click the **Connect** button manually any time that you wish to connect to the Internet.
- **Domain Name Service:** Select **Get Automatically from ISP** if the ISP will provide the DNS address, if not, select **Use these DNS servers** and specify the primary and secondary DNS server IP address.
- Click on the **Apply** button to save the changes.

#### 7.4.1.4 WAN – PPTP

- The WAN interface can be configured as PPTP. This type of connection is usually used for a DSL service and requires a username and password to connect.

[Home](#)
[Reset](#)

### WAN Settings

Internet Connection Type	PPTP
--------------------------	------

Options

MTU	Auto 1460
-----	-----------

PPTP Options

IP Address	10 . 1 . 1 . 10
Subnet Mask	255 . 255 . 0 . 0
Default Gateway	10 . 1 . 1 . 15
PPTP Server	0 . 0 . 0 . 0
Username	
Password	

☐ Connect on Demand: Max Idle Time 15 Minutes  
☒ Keep Alive: Redial Period 30 Seconds

Domain Name Server (DNS) Address

☒ Get Automatically From ISP  
☐ Use These DNS Servers

Primary DNS	0 . 0 . 0 . 0
Secondary DNS	0 . 0 . 0 . 0

[Apply](#)
[Cancel](#)

- Internet Connection Type:** Select **PPPoE** from the drop-down list.
- MTU:** The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.
- PPTP Options:** Specify IP address, subnet mask, default gateway and PPTP server.
- Username:** Specify the user name which is provided by your ISP.
- Password:** Specify the password which is provided by your ISP, and then verify it once again in the next field.
- Type:** Select a reconnection type: **Keep Alive** (A connection to the Internet is always maintained), **Connect on Demand:** You have to open up the Web-based management

- interface and click the **Connect** button manually any time that you wish to connect to the Internet.
- **Domain Name Service:** Select **Get Automatically from ISP** if the ISP will provide the DNS address, if not, select **Use these DNS servers** and specify the primary and secondary DNS server IP address.
  - Click on the **Apply** button to save the changes.

### 7.4.2 LAN Settings

Click on the **LAN Settings** link under the **Router** drop-down menu. This page allows you to configure the LAN interface as IP address, IP subnet mask and WINS server IP. When you enable 'Use Router As DHCP Server', specify the IP address from starting to ending.

**LAN Settings**

HomeReset

**LAN IP Setup**

IP Address	19 . 16 . 1 . 1
IP Subnet Mask	25 . 25 . 25 . 0
WINS Server IP	0 . 0 . 0 . 0

☒ Use Router As DHCP Server

Starting IP Address	19 . 16 . 1 . 2
Ending IP Address	19 . 16 . 1 . 25

ApplyCancel

### 7.4.3 VPN Pass Through

- Click on the **VPN Pass Through** link under the **Router** drop-down menu. This page allows you to enable the pass through feature.

**VPN Pass Through**

HomeReset

☒ PPTP Pass Through  
☒ L2TP Pass Through  
☒ IPSec Pass Through

ApplyCancel

- **PPTP Pass Through:** Place a check in this box if you would like to enable this pass through. PPTP is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels"

- **L2TP Pass Through:** Place a check in this box if you would like to enable this pass through. Layer 2 Tunneling Protocol is a transport protocol that enables tunneling through the Internet for the establishment of virtual private networks.
- **IPSec Pass Through:** Place a check in this box if you would like to enable this pass through. IPSec is a VPN protocol used to implement secure exchange of packets at the IP layer.
- Click on the **Apply** button to save the changes.

## 7.5 Wireless

### Wireless

- Wireless Network
- Wireless Security
- Wireless Advanced Settings

- Click on the **Wireless** link on the navigation drop-down menu. You will then see three options: wireless network, wireless security, and wireless advanced settings. Each option is described below.

### 7.5.1 Wireless Network

- The **Wireless Network** page allows you to configure the wireless mode, channel, SSID, and security settings.

#### Wireless Network

Home

Reset

Wireless Mode	802.11b/g Mixed (2GHz/54Mbps) ▾
SSID	Specify the static SSID : <input type="text" value="EnGenius"/> ( 1 to 32 characters ) Or press the button to search for any available WLAN Service. <input type="button" value="Site Survey"/>
Prefer BSSID	<input type="checkbox"/> <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>

Apply

Cancel

- **Wireless Mode:** Depending on the type of wireless clients that are connected to the network, you may select **B**, **G**, or **B/G-mixed**. If you are not sure about which clients will be accessing the wireless networks, it is recommended that you select **B/G-mixed** for the best performance.
- **SSID:** The SSID is a unique named shared amongst all the points of the wireless network. The SSID must be identical on all points of the wireless network and cannot exceed 32 characters. You may specify an SSID or select one from the **Site Survey**.
- **Site Survey:** Click on the **Site Survey** button in order to scan the 2.4GHz frequency for devices that broadcast their SSID. Click on the **BSSID** link to connect to the Access Point. Click on the **Refresh** button to re-scan the frequency.

#### Site Survey

##### 2.4GHz Site Survey

☒ Infrastructure
 ☐ Ad\_hoc

BSSID	SSID	Channel	Signal	Type	Security	Network Mode
00:e0:4c:81:86:21	DinoNet	1	-86 dBm	B	WEP	<input checked="" type="radio"/>
00:13:d7:7c:6f:43	SMC	6	-105 dBm	G	NONE	<input type="radio"/>

Refresh



## 7.5.2 Wireless Security

### Wireless Security

[Home](#)[Reset](#)

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode

Disabled

[Apply](#)[Cancel](#)

#### 7.5.2.1 Wireless Security : WEP

- **Security Mode:** Select **WEP** from the drop-down list if your wireless network uses WEP encryption. WEP is an acronym for Wired Equivalent Privacy, and is a security protocol that provides the same level of security for wireless networks as for a wired network.

### Wireless Security

[Home](#)[Reset](#)

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode

WEP

Auth Type

Open System

Input Type

Hex

Key Length

40/64-bit (10 hex digits or 5 ASCII char)

Default Key

1

Key1

Key2

Key3

Key4

[Apply](#)[Cancel](#)

- **Authentication Type:** Select an authentication method. Options available are **Open Key**, **Shared Key**. An open system allows any client to authenticate as long as it conforms to any MAC address filter policies that may have been set. All authentication packets are transmitted without encryption. Shared Key sends an unencrypted challenge text string to any device attempting to communicate with the Access Point. The device requesting authentication encrypts the challenge text and sends it back to the Access Point. If the challenge text is encrypted correctly, the Access Point allows the requesting device to authenticate. It is recommended to select Auto if you are not sure which authentication type is used.
- **Input Type:** Select Hex or ASCII from the drop-down list
- **Key Length:** Select a key format from the drop-down list. 64bit-hex keys require 10 characters, where as 128-bit keys require 26 characters. A hex key is defined as a number between 0 through 9 and letter between A through F and a through f.

- **Default Key:** You may use up to four different keys for four different networks. Select the current key that will be used.
- **Key 1-4:** You may enter four different WEP keys.
- Click on the **Apply** button to save the changes.

### 7.5.2.2 Wireless Security : WPA-PSK, WPA2-PSK,

- **Security Mode:** Select **WPA-PSK** or **WPA2-PSK** from the drop-down list if your wireless network uses WPA pre-shared key.

**Wireless Security** [Home](#) [Reset](#)

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA-PSK
Encryption	TKIP
Passphrase	<input type="text"/> (8 to 63 characters) or (64 Hexadecimal characters)

[Apply](#) [Cancel](#)

**Wireless Security** [Home](#) [Reset](#)

Changing the wireless security settings may cause this wireless client to associate with a different one. This may temporarily disrupt your configuration session.

Security Mode	WPA2-PSK
Encryption	TKIP
Passphrase	<input type="text"/> (8 to 63 characters) or (64 Hexadecimal characters)

[Apply](#) [Cancel](#)

- **Encryption:** Select **TKIP** or **AES** from the drop-down list if your wireless network uses this encryption. WPA (Wi-Fi Protected Access) was designed to improve upon the security features of WEP (Wired Equivalent Privacy). The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. WPA provides improved data encryption through the Temporal Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and by adding an integrity checking feature which makes sure that keys haven't been tampered with.
- **Passphrase:** Specify a passphrase that is shared amongst the Access Points and clients.
- Click on the **Apply** button to save the changes.

### 7.5.3 Wireless Advanced Settings

- Click on the **Wireless Advanced Settings** link. On this page you can configure the advanced settings to tweak the performance of your wireless network. Options available are: data rate, transmit power, fragmentation threshold, RTS threshold, protection mode and distance.

**Wireless Advanced Settings**[Home](#)[Reset](#)

Data Rate	Auto
Transmit Power	20 dBm
Fragment Length (256 - 2346)	2346 bytes
RTS/CTS Threshold (1 - 2346)	2346 bytes
Protection Mode	Disable
WMM	Disable
Channel Bandwidth	20MHz
Distance (1-30km)	1 km

[Apply](#)[Cancel](#)

- **Data Rate:** If you would like to force a data rate, you may select one from the drop-down list. However, for best performance it is recommended to use the **Auto** setting.
- **Transmit Power:** You may have the different application distance of the device by selecting a value from the drop-down list. This feature can be helpful in restricting the coverage area of the wireless network.
- **Fragment:** Packets over the specified size will be fragmented in order to improve performance on noisy networks.
- **RTS Threshold:** Packets over the specified size will use the RTS/CTS mechanism to maintain performance in noisy networks and preventing hidden nodes from degrading the performance.
- **Protection Mode:** If your wireless network is using both 802.11b and 802.g devices then it is recommended to enable this feature so that the 802.11b devices will not degrade the performance of 802.11g devices.
- **WMM:** Enable wireless Quality of Service
- **Distance (1-30km):** Specify a distance between 1 and 30Km.
- Click on the **Apply** button to save the changes.

**7.6 Management****Management**

- Administration
- SNMP Settings
- Backup/Restore Settings
- Firmware Upgrade
- Time Settings
- Log
- Diagnostics

- Click on the **Management** link on the navigation drop-down menu. You will then see six options: administration, SNMP settings, backup/restore settings, firmware upgrade, time settings, log and Diagnostics. Each option is described below.

### 7.6.1 Administration

- Click on the **Administration** link under the **Management** menu. This option allows you to create a user name and password for the device. By default, this device is configured without a user name and password **admin**. For security reasons it is highly recommended that you create a new user name and password.

**Administration** [Home](#) [Reset](#)

**Administrator**

Name	admin
Password	*****
Confirm Password	*****

**Remote Access**

Remote Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote Upgrade	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Remote Management Port	8080

[Apply](#) [Cancel](#)

- Name:** Specify a user name into the first field.
- Password:** Specify a password into this field and then re-type the password into the **Confirm Password** field.
- Remote Management:** Choose to enable or disable remote management.
- Remote Upgrade:** Choose to enable or disable remote firmware upgrade.
- Remote Management Port:** Specify a port for remote management. For example, if you specify 8080, then you will need to specify <IP address>:<port> 192.168.1.1:8080 to connect to the web interface of the device.
- Click on the **Apply** button to save the changes.

### 7.6.2 SNMP Settings

- Click on the **SNMP Settings** link under the **Management** menu. This option allows you to assign the contact details, location, and community name and trap settings for SNMP. This is a networking management protocol used to monitor network-attached devices. SNMP allows messages (called protocol data units) to be sent to various parts of a network. Upon receiving these messages, SNMP-compatible devices (called agents) return data stored in their Management Information Bases. .

## SNMP Settings

[Home](#)[Reset](#)

SNMP Enable/Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Community Name (Read Only)	<input type="text" value="public"/>
Community Name (Read/Write)	<input type="text" value="private"/>
Trap Destination IP Address	<input type="text" value="0 . 0 . 0 . 0"/>
Trap Destination Community Name	<input type="text" value="public"/>

[Apply](#)[Cancel](#)

- **SNMP Enable/Disable:** Choose to **enable** or **disable** the SNMP feature.
- **Contact:** Specify the contact details of the device.
- **Location:** Specify the location of the device.
- **Read-Only Community Name:** Specify the password for access the SNMP community for read only access.
- **Read-Write Community Name:** Specify the password for access to the SNMP community with read/write access.
- **Trap Destination IP Address:** Specify the IP address of the computer that will receive the SNMP traps.
- **Trap Destination Community Name:** Specify the password for the SNMP trap community.
- Click on the **Apply** button to save the changes.

### 7.6.3 Backup/Restore settings, Reset to factory default settings

- Click on the **Backup/Restore Setting** link under the **Management** menu. This option is used to save the current settings of the device in a file on your local disk or load settings on to the device from a local disk. This feature is very handy for administrators who have several devices that need to be configured with the same settings.

## Backup/Restore Settings

[Home](#)[Reset](#)

Save A Copy of Current Settings	<a href="#">Backup</a>
Restore Saved Settings from A File	<a href="#">選擇檔案</a> <a href="#">尚未選取檔案</a> <a href="#">Restore</a>
Revert to Factory Default Settings	<a href="#">Factory Default</a>

- **Save a copy of the current settings:** Click on the Backup button to save the current configuration.

- **Restore saved settings from a file:** Once a file has been backed up, you may restore it by clicking on the Browse button to select the file, and then the **Restore** button.
- **Revert to factory default settings:** Click on the Factory Default Settings button to reset the device to the default settings. Please wait while the device restart and then access the device using the default IP address: 192.168.1.1

#### System Rebooting...

Rebooting, Please wait... 

[Click here when AP is ready](#)

### 7.6.4 Firmware Upgrade

- Click on the **Upgrade Firmware** link under the **Management** menu. This page is used to upgrade the firmware on the device. Make sure that downloaded the appropriate firmware from your vendor.

**Firmware Upgrade**

HomeReset

Current firmware version: 1.0.39

Locate and select the upgrade file from your hard disk:

選擇檔案

尚未選取檔案

Upgrade

- Click on the **Browse** button and then select the appropriate firmware and then click on the **Upgrade** button.

**Note:** The upgrade process may take about 1 minute to complete. Do not power off the device during this process as it may crash the device and make it unusable. The device will restart automatically once the upgrade is complete.

### 7.6.5 Time Settings

- Click on the **Time Settings** link under the **Management** menu. This page allows you to configure the time on the device. You may do this manually or by connecting to a NTP server.

**Time Settings**

HomeReset

Time

☒ Manually Set Date and Time

2000 / 01 / 01 01 : 18

☐ Automatically Get Date and Time

Time Zone: UTC+00:00 England

☐ User defined NTP Server: 0 . 0 . 0 . 0

ApplyCancel

- **Manually Set Date and Time:** Specify the date and time
- **Automatically Get Date and Time:** Select the time zone from the drop down list and then specify the IP address of the NTP server.
- Click on the **Apply** button to save the changes.

### 7.6.6 Log

- Click on the **Log** link under the **Management** menu. The **Log** page displays a list of events that are triggered on the Ethernet and Wireless interface. This log can be referred when an unknown error occurs on the system or when a report needs to be sent to the technical support department for debugging purposes.

**Log**

HomeReset

**Syslog**

Syslog

Disable

Log Server IP Address

0 . 0 . 0 . 0

**Local log**

Local Log

Disable

Apply

Cancel

- **Syslog:** Choose to enable or disable the system log.
- **Log Server IP Address:** Specify the IP address of the server that will receive the system log.
- **Local Log:** Choose to enable or disable the local log.
- Click on the **Apply** button to save the changes.

### 7.6.7 Diagnostics

- Click on the **Diagnostics** link under the **Management** menu. In this page, user can let unit to ping other network equipment. And user also can monitor a route from unit to your target.

**Diagnostics**

HomeReset

**Ping Test Parameters**

Target IP

Ping Size

64

Bytes

Number of Pings

4

Start Ping

**Traceroute Test Parameters**

Traceroute target

Start Traceroute

- **Ping Test Parameters** : User can input Target IP, Ping Size and Ping Quantity of other network device which connected you want. And then you can find the ping condition after click **Start Ping**.
- **Traceroute Test Parameters**: This function help user to monitor a network trace. User can input IP or domain name on Traceroute target.



## Appendix A – FCC Interference Statement

---

### Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### IMPORTANT NOTE:

#### FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

## Appendix B – IC Statement

---

### **Industry Canada statement:**

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

### **IMPORTANT NOTE:**

#### **Radiation Exposure Statement:**

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This device has been designed to operate with an antenna having a maximum gain of 5 dBi. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.